



Operating System

Advanced Certificate Management

Beta 3 Technical Walkthrough

Abstract

This technical walkthrough takes you through the process that administrators go through to obtain and manage certificates in the Microsoft® Windows® 2000 operating system, using the Certificates Microsoft Management Console (MMC) snap-in. End-user scenarios are covered in a separate walkthrough.

© 1999 Microsoft Corporation. All rights reserved.

THIS IS PRELIMINARY DOCUMENTATION. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This BETA document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, the BackOffice logo, Windows, and Windows NT are registered trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

*Microsoft Corporation • One Microsoft Way • Redmond, WA 98052 -6399 • USA
0499*

CONTENTS

INTRODUCTION	1
Prerequisites	1
ADVANCED CERTIFICATE MANAGEMENT IN WINDOWS 2000.	2
Managing User Certificates	2
Obtaining a Certificate from a Certification Authority on Your Windows 2000 Domain	4
Viewing a Certificate	8
Exporting Certificates	13
Importing Certificates	18
Connecting to a Computer	23
FOR MORE INFORMATION	28
Before You Call for Support	28
Reporting Problems	28

INTRODUCTION

This technical walkthrough takes you through the process that administrators would go through to obtain and manage certificates in Microsoft Windows® 2000 using the Certificates Microsoft Management Console (MMC) snap-in. End-user scenarios are covered in a separate walkthrough.

Prerequisites

This technical walkthrough assumes the following environment:

- You are using Windows 2000 build 1943 or later in a Windows 2000 domain.
- You are a domain administrator or the administrator of the local computer.
- There is a Windows 2000 Certification Authority running Enterprise policy in the domain.

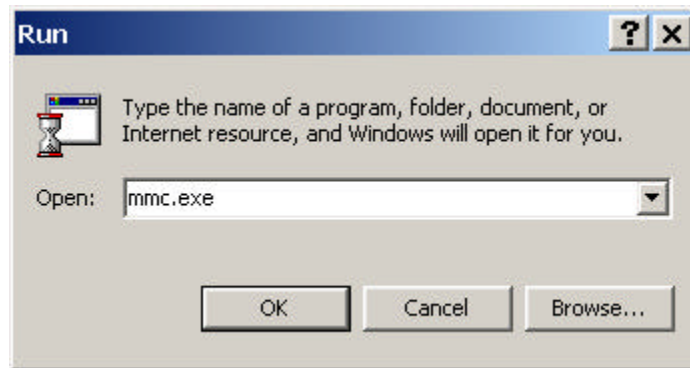
ADVANCED CERTIFICATE MANAGEMENT IN WINDOWS 2000

Managing User Certificates

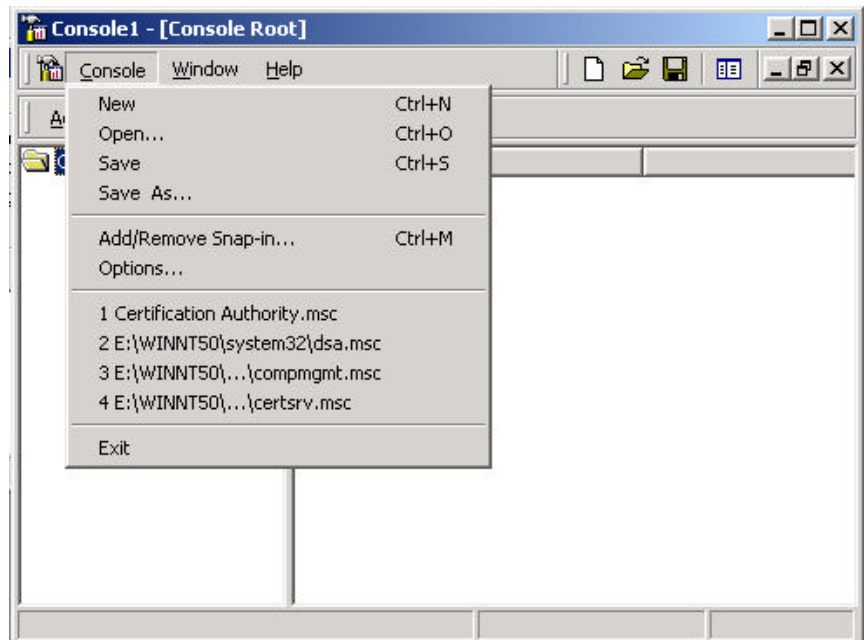
This section explains how to use the Certificates MMC snapin to manage certificates.

To start the Certificates MMC snapin

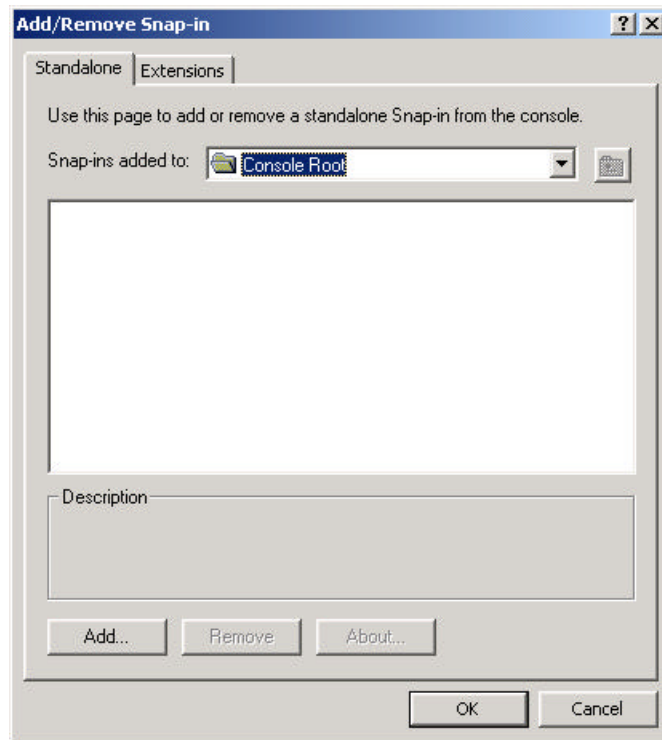
1. Start the MMC: from the **Start** menu, click **Run**. Type **mmc** and click **OK**.



2. On the **Console** menu, click **Add/Remove Snap-in**.



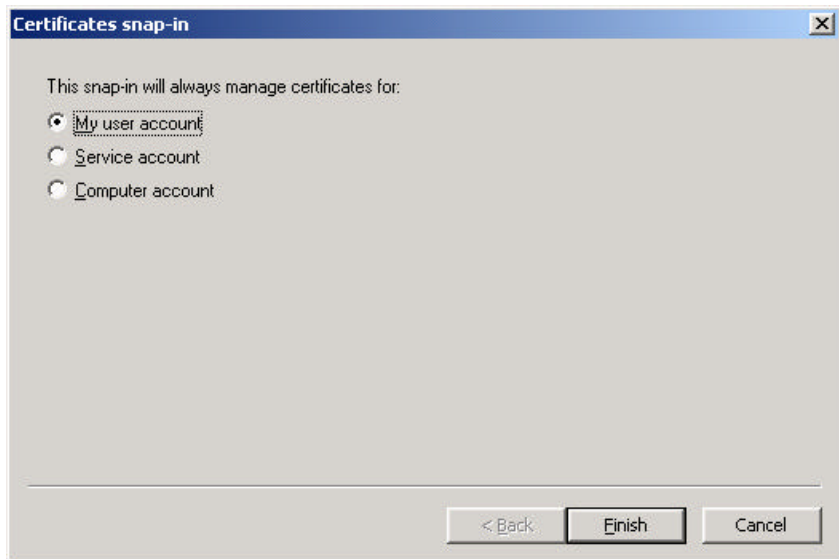
3. Click **Add** to add a snap-in to the current console.



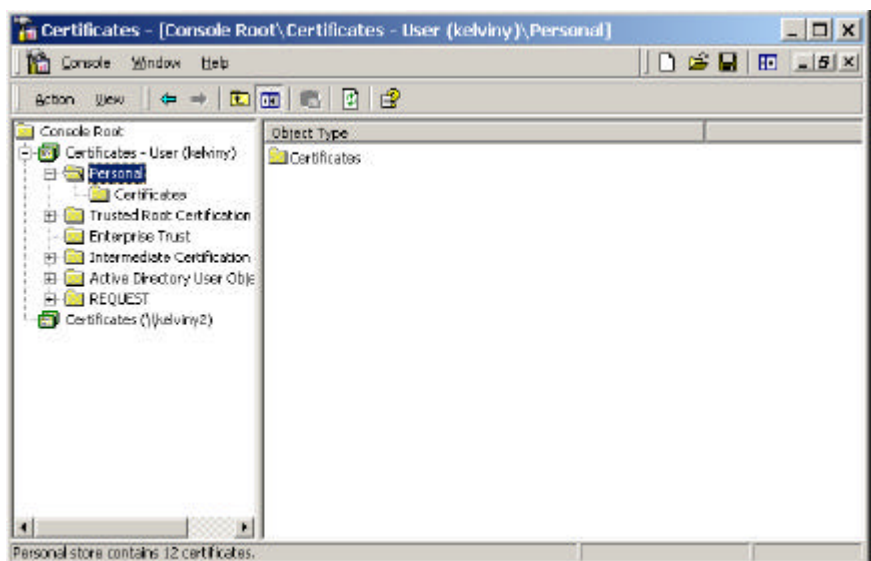
4. Select **Certificates** and click **Close**.



5. Select **My user account**. Click **Finish**.



6. Click **OK** to close the **Add/Remove Snap-in** dialog.

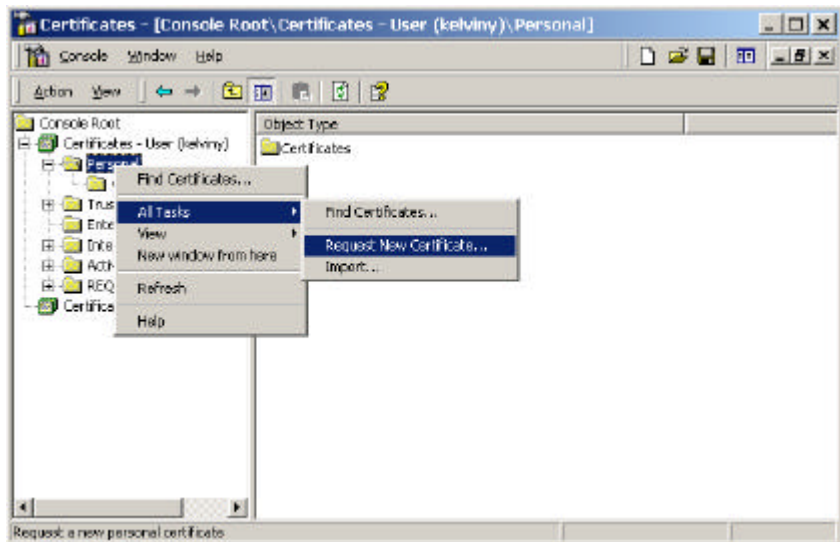


Obtaining a Certificate from a Certification Authority on Your Windows 2000 Domain

This process requires a certification authority installed in the same Windows 2000 domain as the client running the Microsoft Certification Authority service. The certification authority must be installed either as a root or subordinate Enterprise Certificate Authority (CA).

To obtain a certificate

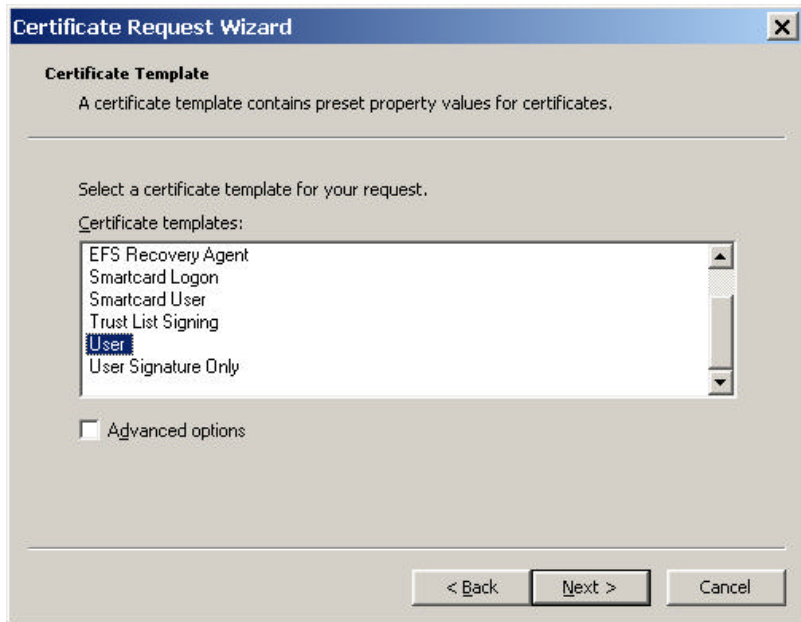
1. Right-click the **Personal** node.



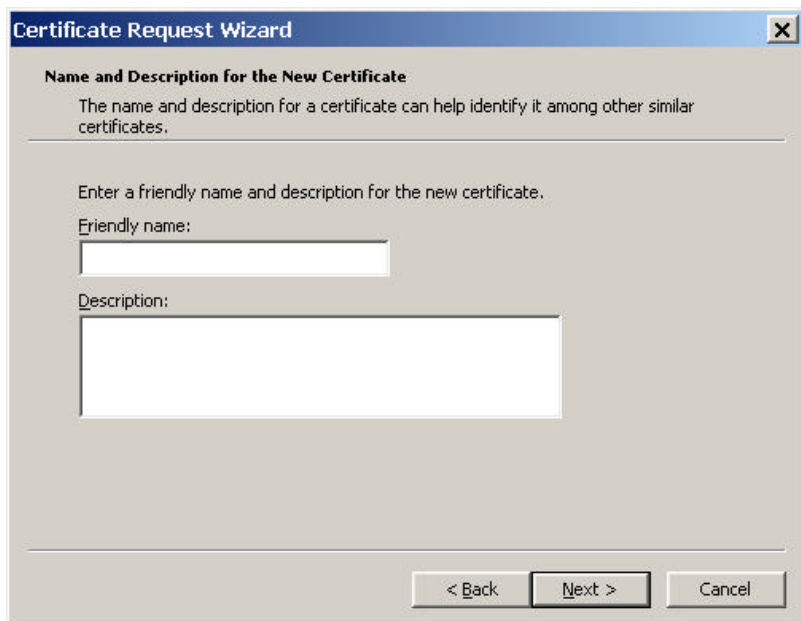
2. On the **All Tasks** submenu, select **Request New Certificate**



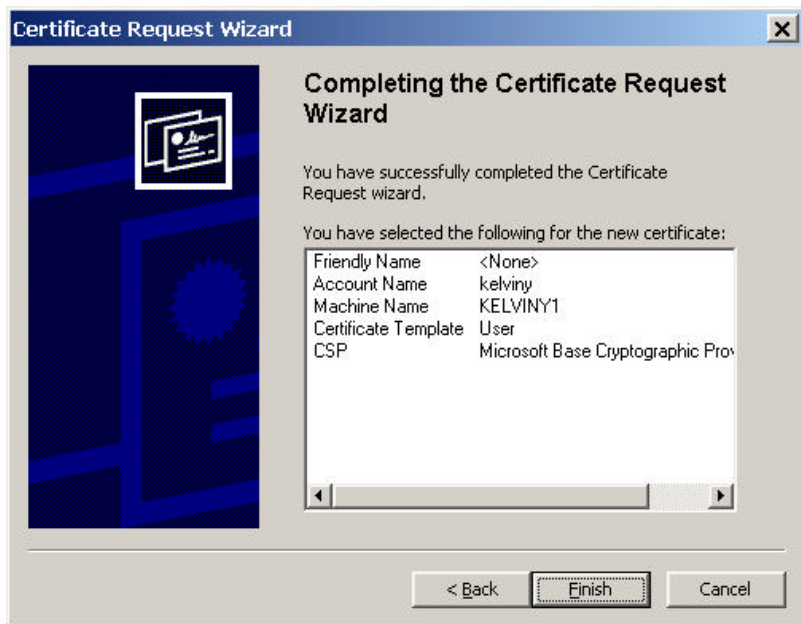
3. Click **Next**.



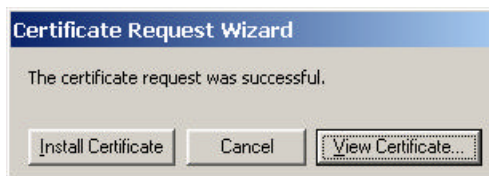
4. Select the certificate template that you want the new certificate to be based on. Click **Next**.



5. Enter a friendly name or a description, if desired. Click **Next**.



- Click **Finish** to send the certificate request to the CA.



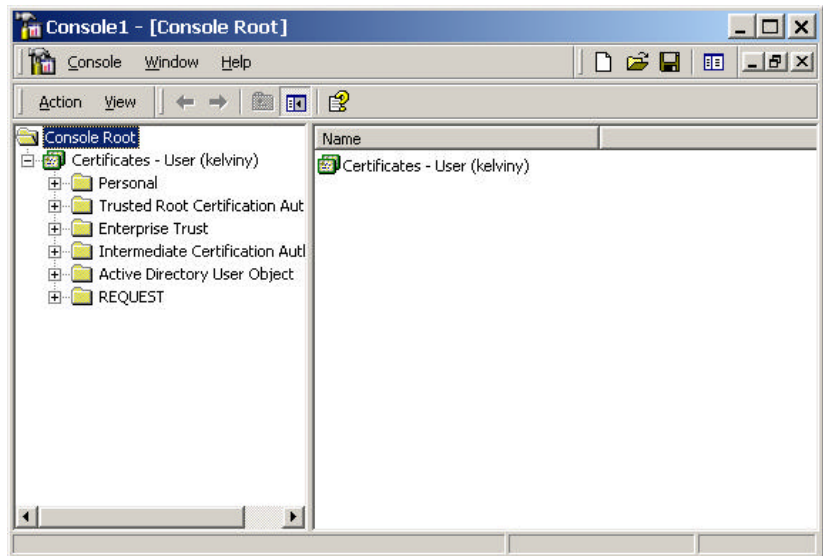
- Click **Install Certificate** to install the certificate to the certificate store. You can also view the certificate before installation by clicking **View Certificate**.

Viewing a Certificate

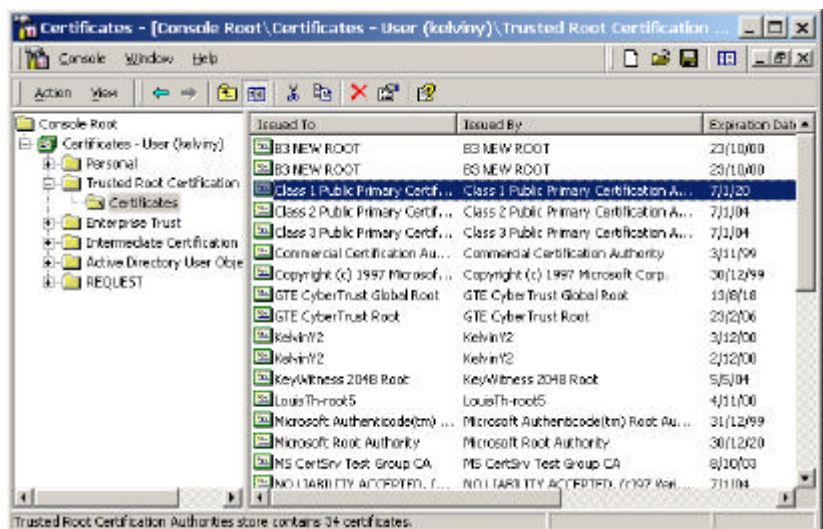
You may need to look at your certificates in the certificate stores.

To view a certificate

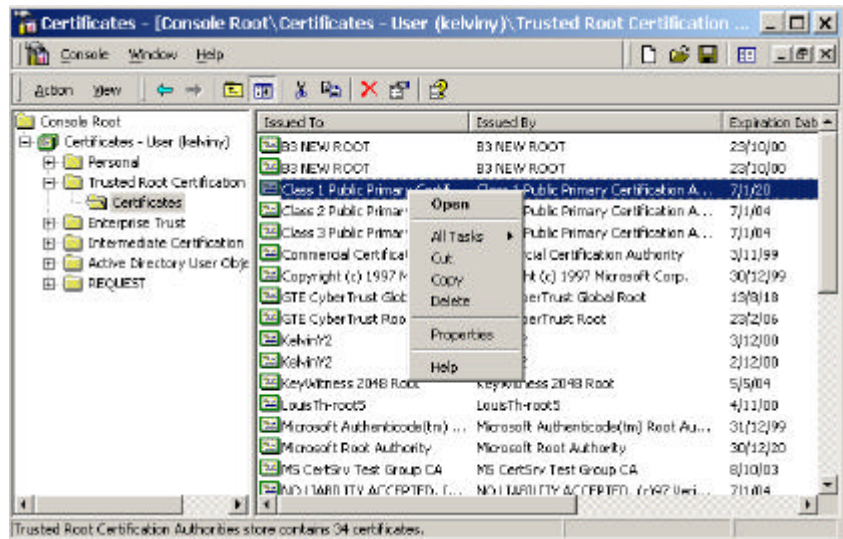
1. Expand the certificate store that contains the certificate you want to view.



2. Click **Certificates** to see the list of certificates in that certificate store.



3. Right-click the certificate that you want to view, then click **Open**. You can also view a certificate by doubleclicking it.

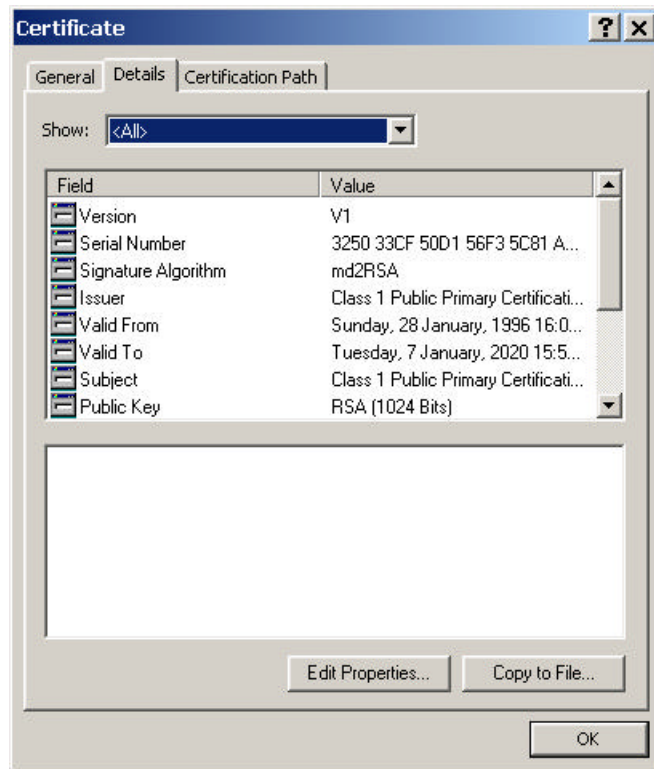


4. The certificate dialog is organized into 3 tabs.

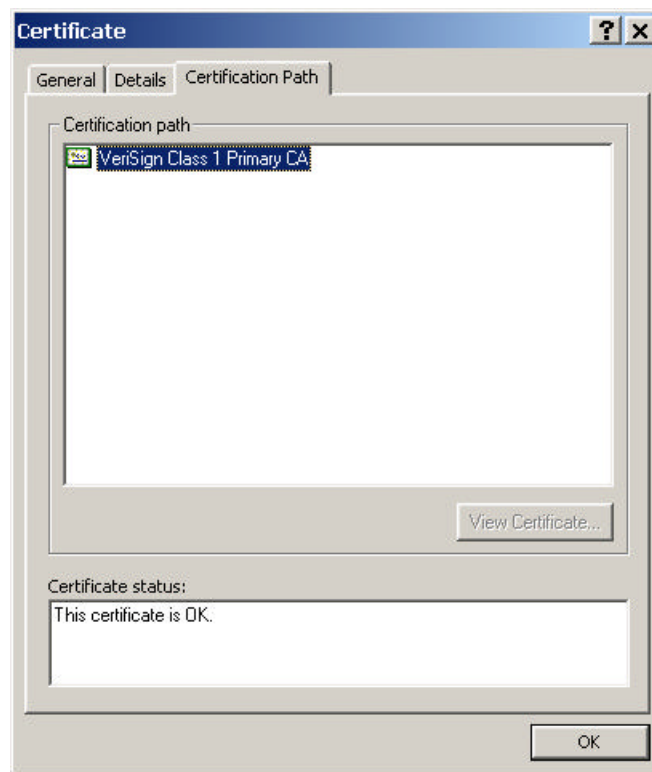
The **General** tab is the default view for seeing a certificate's uses.



The *Details* tab displays the actual X.509 fields, extensions, and properties of a certificate. You may also click **Edit Properties** in this view, which allows you to modify the Friendly Name and Description fields. You can also specify what the certificate can be used for.



The Certification Path tab displays the certification path.



Exporting Certificates

You may backup important certificates and the corresponding private keys, or move them to another computer.

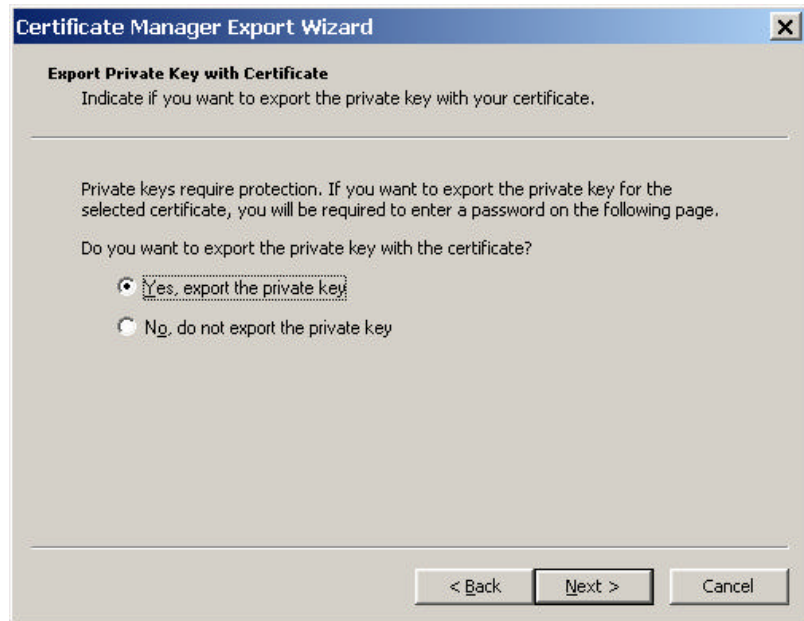
To export certificates

1. Right-click the certificate(s) you want to export.
2. On the **Task** submenu, click **Export** to launch the Certificate Manager Export Wizard. Click **Next**.

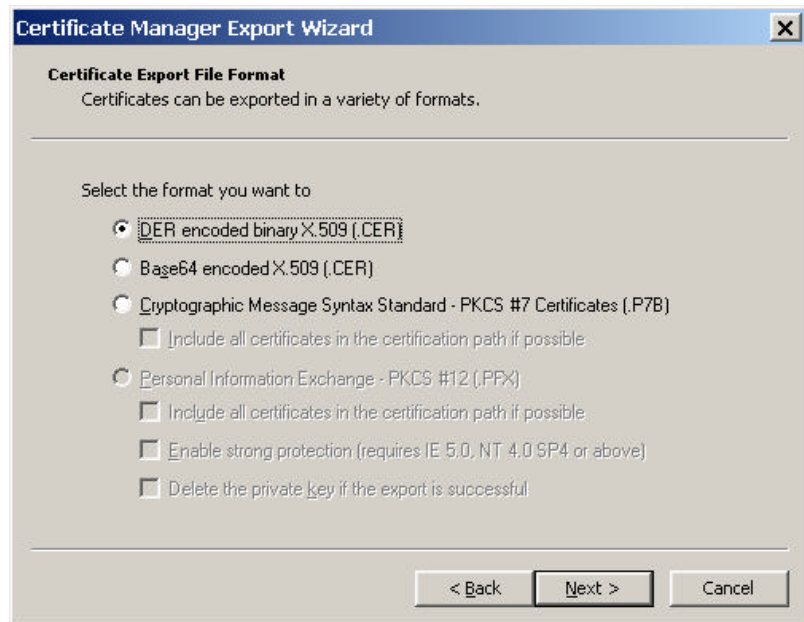


3. If the certificate that you are exporting has a corresponding private key in the system, you can choose to export the private key with the certificate.

Note You will only be able to export to a Personal Information Exchange PKCS#12 file if you want to export the private key.



4. Select the export file format. Click **Next**.

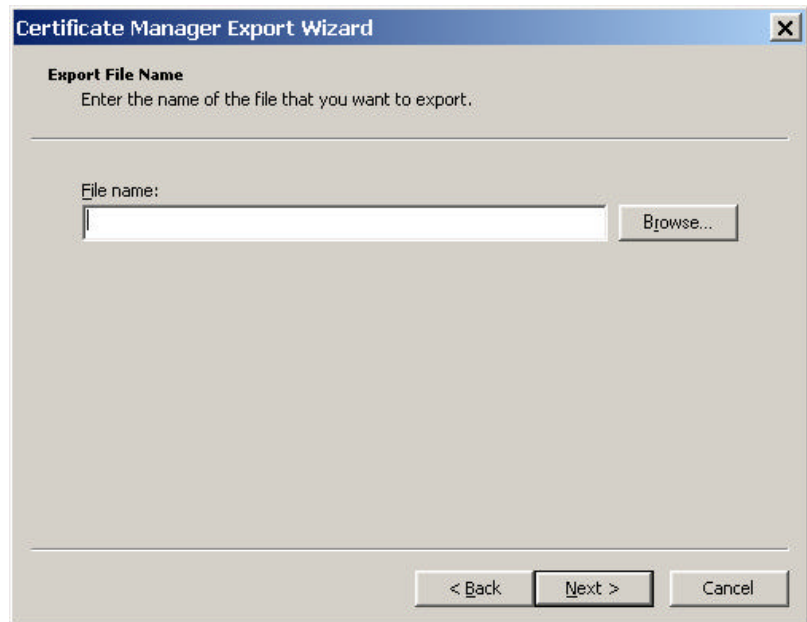


5. If the file specified is a Personal Information Exchange—PKCS #12 (*.pfx), you will be prompted for the password. Enter the password to import the file. Click **Next**.



The image shows a Windows dialog box titled "Certificate Manager Export Wizard". The main heading is "Password Protection for the Private Key". Below this, a message states: "To maintain security, the private key is secret and must be protected with a password." A horizontal line separates this from the next section, which says: "Enter a password to encrypt the private key you are exporting." There are two text input fields: the first is labeled "Password:" and the second is labeled "Confirm password:". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

6. Enter the name of the file you want to export. Click **Next**.



The image shows a Windows dialog box titled "Certificate Manager Export Wizard". The dialog has a blue title bar with a close button (X) in the top right corner. The main area is light gray and contains the following elements:

- Export File Name**: A section header in bold.
- Enter the name of the file that you want to export.**: A line of instructional text.
- File name:**: A label for the text input field.
- : A text input field for the file name.
- Browse...**: A button to the right of the text input field.
- < Back**, **Next >**, and **Cancel**: Three buttons at the bottom right of the dialog.

7. Verify the choices you have made in the wizard. Click **Finish** to export to the file.



Importing Certificates

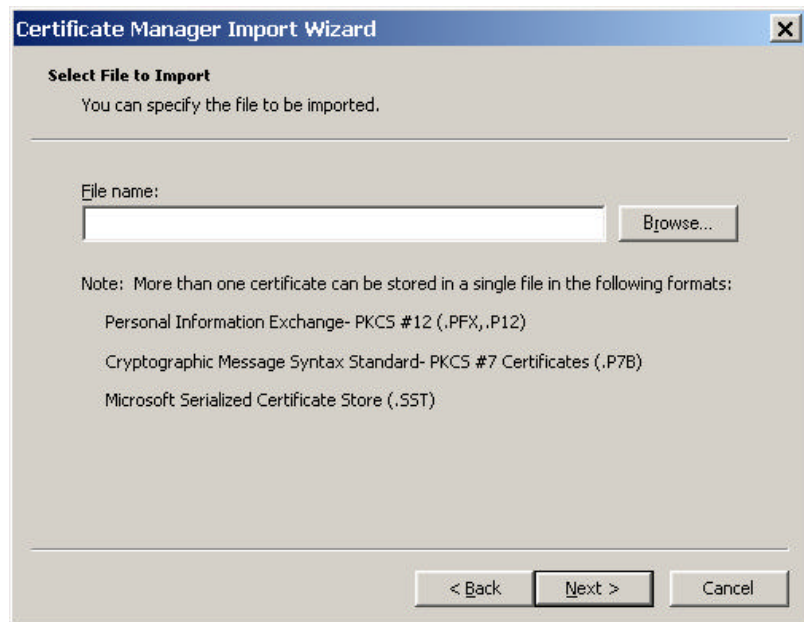
You may restore certificates and the corresponding private keys from a file.

To import a file

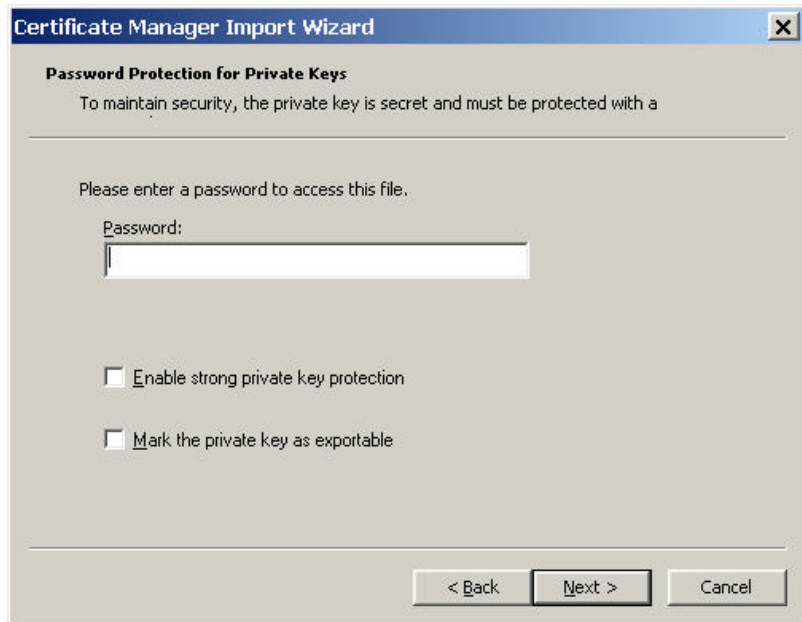
1. Right-click the certificate store you want to import.
2. On the **Task** submenu, click **Import** to launch the Certificate Manager Import Wizard. Click **Next**.



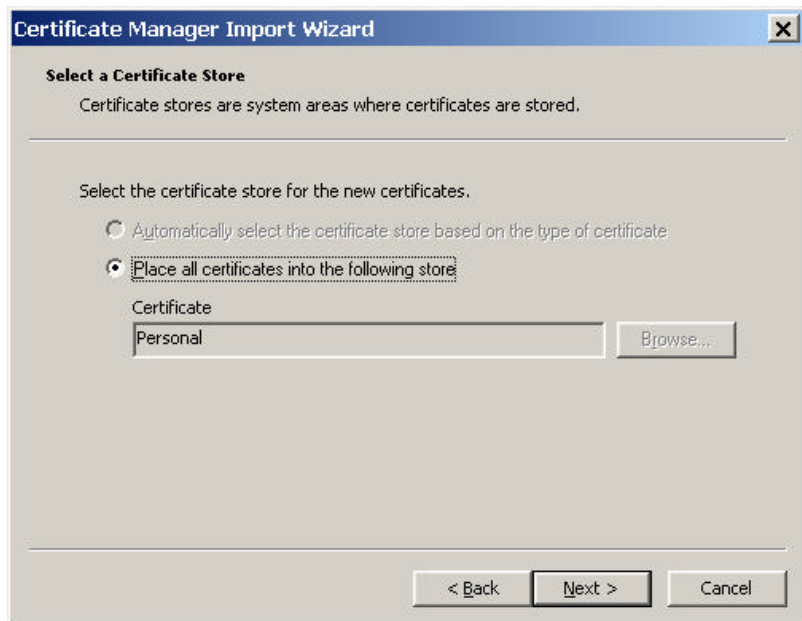
3. Type the name of the certificate file that you want to import. Alternatively, you may find the file by clicking **Browse**. Click **Next**.



4. If the file specified is a Personal Information ExchangePKCS #12 (*.pfx), you will be prompted for the password. Enter the password to import the file. Click **Next**.



5. Click **Next** to continue.



6. The next wizard page contains summary information about the file that you are importing. Click **Finish** to import the file. The certificate(s) are now ready for use by the system.

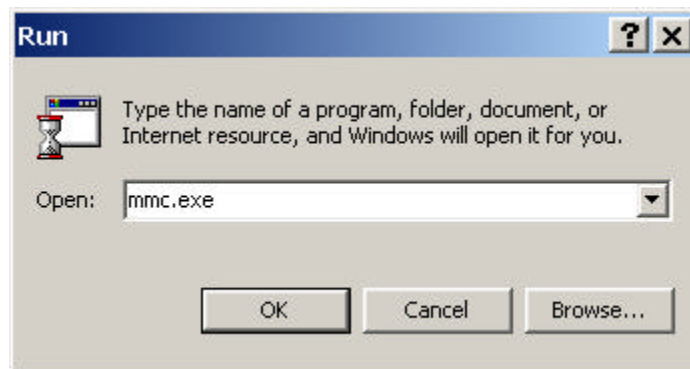


Connecting to a Computer

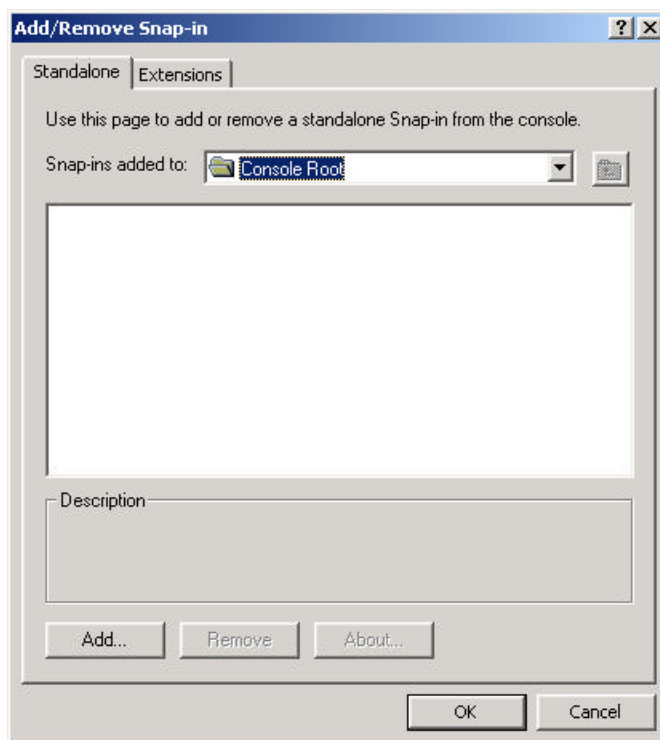
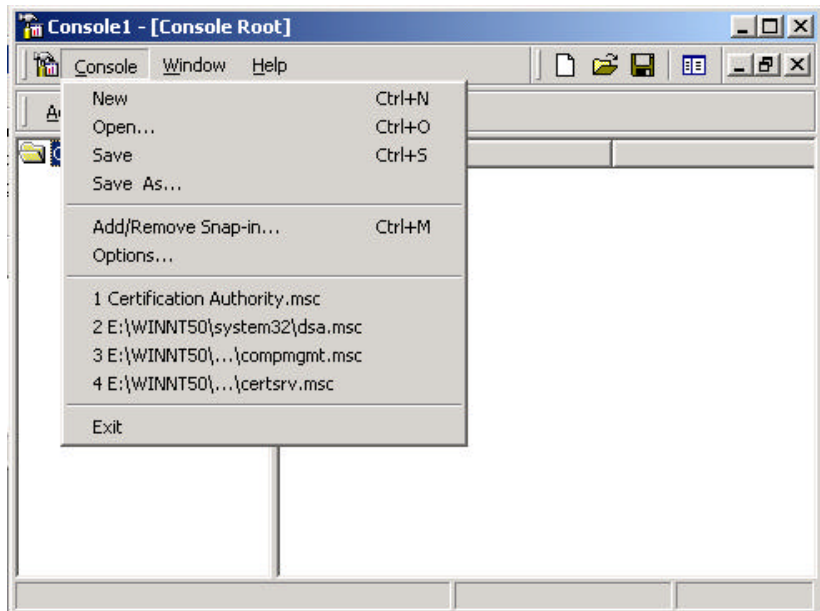
The Certificates MMC snapin can be used to manage a computer's certificates.

To connect to a computer

1. Start the MMC by clicking **Run** on the **Start** menu. Then type in *mmc.exe* and click **OK**.



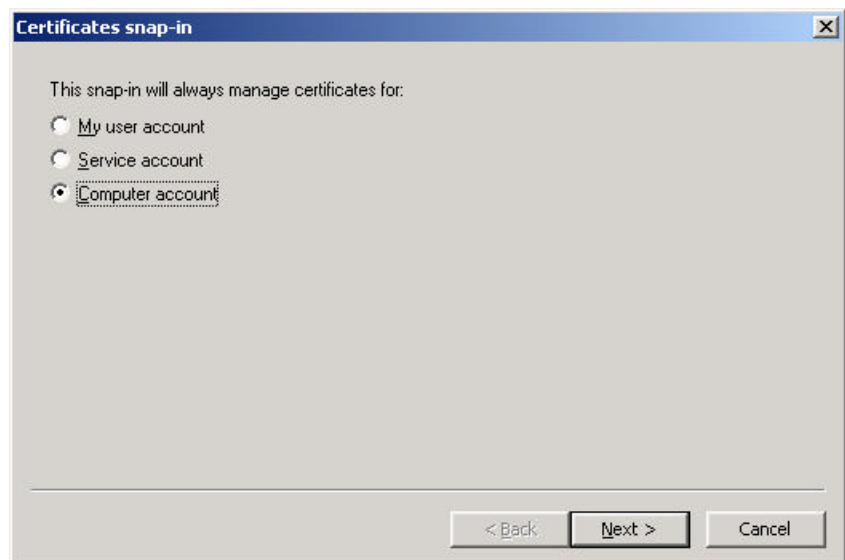
2. On the **Console** menu, click **Add/Remove Snap-in**.



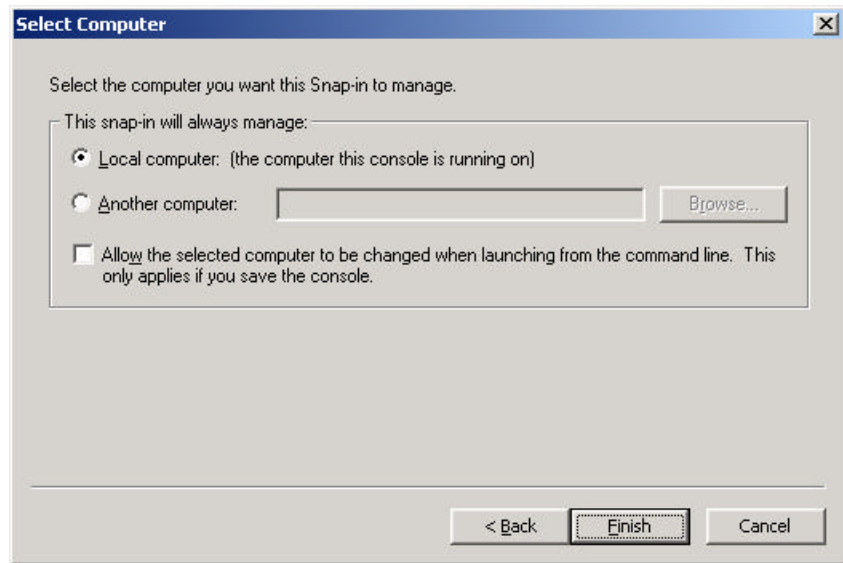
3. Click **Add** to add a snap-in to the current console.



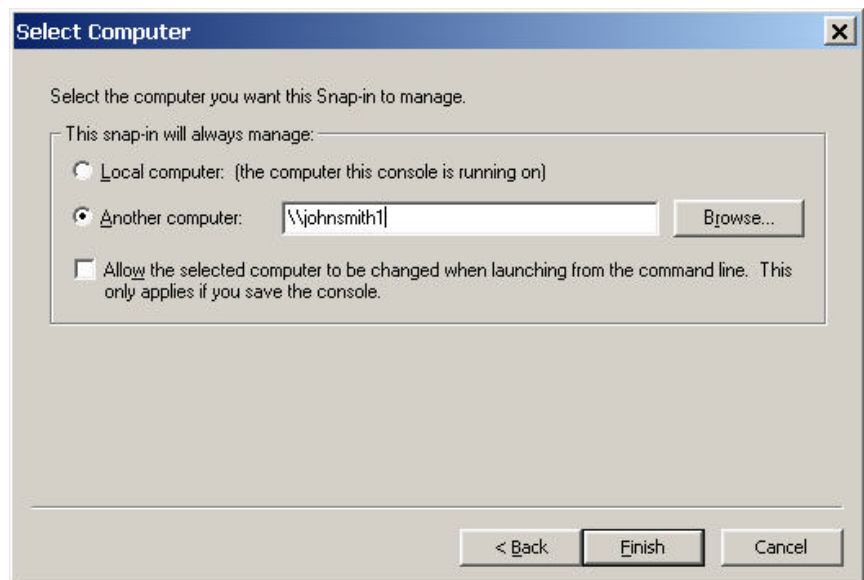
4. Select **Certificates** and then click **Add**.



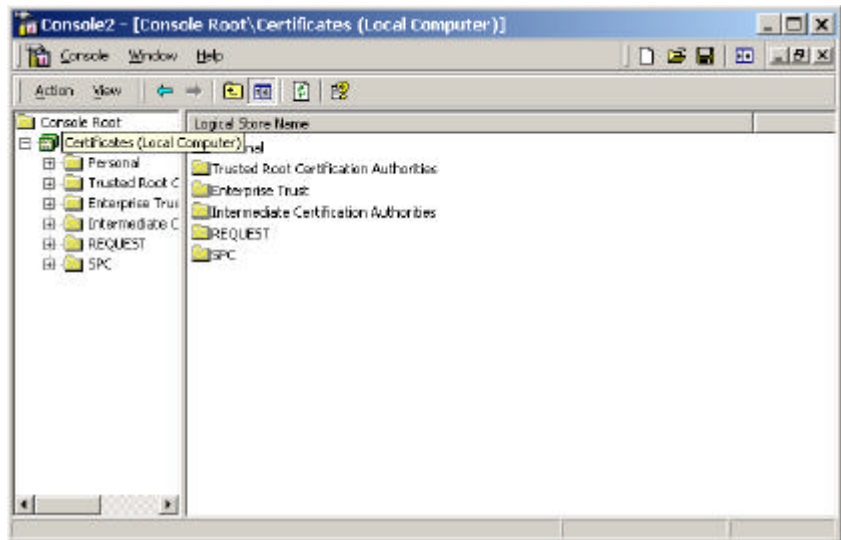
5. Click **Computer account** and then click **Next**.



6. Click the radio button for **Another computer**. Type the name of the computer you want to manage (or click **Browse** to select from a list). Click **Finish**.



7. Click **OK** to close the **Add/Remove Snap-in** dialog box.



FOR MORE INFORMATION

For the latest information on Microsoft Windows2000 network operating system, visit our World Wide Web site at <http://www.microsoft.com/windows/server/> and the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

For the latest information on the Windows2000 Beta 3, visit the World Wide Web site at <http://ntbeta.microsoft.com/>.

Before You Call for Support

Please keep in mind that Microsoft does not support these walkthroughs. The purpose of the walkthroughs is to facilitate your initial evaluation of the Microsoft Windows 2000 features. For this reason, Microsoft cannot respond to questions you might have regarding specific steps and instructions.

Reporting Problems

Problems with Microsoft Windows 2000 Beta 3 should be reported via the appropriate bug reporting channel and alias. Please make sure to adequately describe the problem so that the testers and developers can reproduce and fix it. Refer to the Release Notes included on the Windows2000 Beta 3 distribution media for some of the known issues.